UNITED STATES OF AMERICA, Plaintiff,

v.

DOMINIC CAPUTO, Defendant

Case No. 3:18-cr-00428-IM
United States District Court, D. Oregon
Filed Nov 06, 2019

Counsel

Billy J. Williams, United States Attorney, and Michelle Holman Kerin, Assistant United States Attorney, 1000 SW Third Avenue, Suite 600, Portland, Oregon 97204-2902. Attorneys for Plaintiff.

Laurie Shertz, 333 SW Taylor Street, Suite 300, Portland, Oregon 97204, and Ryan O'Connor, 1500 SW First Avenue, Suite 1090, Portland, Oregon 97201. Attorneys for Defendant.

Immergut, Karin J., United States District Judge

OPINION AND ORDER

*1 Defendant was indicted on four counts of wire fraud, in violation of 18 U.S.C. § 1343, and one count of making a false statement in a document, in violation of 18 U.S.C. § 1001(a)(3). ECF 1. On September 10, 2019, Defendant filed a motion to suppress emails and evidence derived from a warrantless search of Defendant's workplace email account. ECF 37. The Government's response to the motion provided additional facts about the email account and the context in which the Government received copies of Defendant's emails. ECF 48. The response included an image of the banner message displayed when Defendant logged on to his work computer system. Id. at 4. The response also attached two policies which governed Defendant's computer use at work. ECF 48-1, 48-2.

On October 15, 2019, this Court held a hearing on the motion to suppress. At the hearing, Defendant's counsel stated that for the purpose of this motion, Defendant stipulates to the facts as presented in Government's response and its attachments. Defendant's counsel also declined the opportunity to present any additional evidence at an evidentiary hearing on the motion. At the end of the hearing, this Court orally denied the motion and indicated that this opinion and order would follow.

BACKGROUND

Since at least September 2011, Defendant worked for the Oregon National Guard in a position subject to computer policies and restrictions established by the U.S. Department of Defense. ECF 48 at 2. The Defense Department conveyed these policies in a banner message displayed each time Defendant logged on to his computer as well through an annual training, the “Cyber Awareness Challenge,” in which Defendant participated. Id. at 2–3, 5. The Department also owned and operated the server that stored and processed Defendant's work emails. Id. at 2.

The indictment concerns the period 2012 through 2014. ECF 1 at 4, 8. During this time, Defendant had to comply with two overlapping computer-use policies as a condition of his employment. ECF 48 at 3. First, he was subject to Army Regulation 25-2 (“AR 25-2”), which was originally issued in October 2007 and revised in March 2009. Id. at 5–6. AR 25-2 specified that using Defense Department computer systems constitutes consent to monitoring and “that there is no expectation of privacy while using [information systems] or accessing Army resources.” ECF 48-2. AR 25-2 also required that a warning banner detailing this information

be displayed each time a user accessed the computer system. Id. The regulation required not only that the warning appear, but also that the user "take a positive action to accept the terms of the notice and consent warning banner before a successful logon is completed." Id. During the period at issue in this case, the warning banner advised:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

*2 - The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

ECF 48 at 4. As AR 25-2 required, see ECF 48-2, this banner appeared each time Defendant logged on to his computer and required that he "acknowledge and consent to [it] in order to gain access to the computer system and perform his job," ECF 48 at 3.

Defendant was also subject to the Oregon National Guard's acceptable use policy. ECF 48 at 3. This policy included conditions identical to those contained in the warning banner. See ECF 48-1 at 3–4. Employees of the Oregon National Guard, including Defendant, were required to sign the policy before they received computer access. ECF 48 at 4. They also had to acknowledge and recertify their understanding of the policy annually. Id. Users who had not recertified within the past year were automatically directed to a website to complete the recertification process. [1] Id. at 5.

STANDARDS

The Fourth Amendment protects individuals from unreasonable searches by the government. See Smith v. Maryland, 442 U.S. 735, 739 (1979). The Supreme Court has defined a "search" as an infringement on an individual's reasonable expectation of privacy. See United States v. Jacobsen, 466 U.S. 109, 113 (1984). Demonstrating a reasonable expectation of privacy requires showing that the individual had a subjective expectation of privacy and that this expectation was objectively reasonable. Smith, 442 U.S. at 740 (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). The defendant bears the burden to prove both of these elements, see United States v. Ziegler, 474 F.3d 1184, 1189 (9th Cir. 2007), commonly referred to as the Katz test, see, e.g., United States v. Jones, 565 U.S. 400, 412 (2012).

Warrantless searches are presumptively unreasonable. Jacobsen, 466 U.S. at 114. "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." Riley v. California, 573 U.S. 373, 382 (2014). The ordinary remedy for an unreasonable search is the exclusionary rule, which prohibits "evidence seized during an unlawful search" from use at trial. See Wong Sun v. United States, 371 U.S. 471, 484 (1963).

DISCUSSION

*3 Defendant contends that under the Katz test, he had a reasonable expectation of privacy in his work email messages. Thus, he moves this Court to suppress his emails and evidence derived from them because the Government obtained them without a warrant. Defendant rightly observes that the Fourth Amendment's protections extend to public employees. O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (plurality opinion); id. at 731–32 (Scalia, J., concurring); id. at 737 (Blackmun, J., dissenting). But because any

expectation of privacy in the email account was objectively unreasonable under the workplace's policies, the motion is denied.

As a preliminary matter, this Court notes that Defendant has not offered any evidence that he had a subjective expectation of privacy in his work email. Generally, to evaluate the subjective prong of the Katz test, the court considers whether the individual's actions showed that he sought "to preserve [something] as private." Smith, 442 U.S. at 740 (quoting Katz, 389 U.S. at 351) (alteration in original). In Ziegler, for example, the Ninth Circuit observed that the "use of a password on [a] computer and the lock on [a] private office door are sufficient evidence of such expectation." 474 F.3d at 1189. Here, however, Defendant offered no evidence suggesting that he believed his work email was private, and at oral argument, he declined the opportunity to provide further evidence at an evidentiary hearing. Arguably, he has not met his burden of satisfying the subjective prong under Katz. See id.

However, even if Defendant had a subjective expectation of privacy in his work email, that expectation would be objectively unreasonable given the facts of this case. Defendant notes correctly that in analyzing the objective prong of the Katz test, courts look to the workplace's policies. ECF 37 at 2. The Supreme Court held in O'Connor that "actual office practices and procedures" and "legitimate regulation" shape the reasonableness of privacy expectations. 480 U.S. at 717–18 (discussing employees' "expectations of privacy in their offices, desks, and file cabinets"). In the context of virtual communication, the Ninth Circuit has observed that merely accessing a network or sharing a computer with others does not render one's expectation of privacy unreasonable. United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007) (citing Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001)). But "privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user." Heckenkamp, 482 F.3d at 1147 (citing United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000)).

The Ninth Circuit has closely analyzed the terms of computer and network-use policies to evaluate whether users' expectations of privacy were objectively reasonable. In Heckenkamp, a student at a public university used his personal computer to connect to the university network. 482 F.3d at 1143, 1147. The court held that the network policy, authorizing only limited monitoring, [2] did not diminish a reasonable expectation of privacy in the files on his hard drive. Id. In contrast, the court held that no reasonable expectation of privacy existed for a defendant who confronted banner notices of monitoring and disclosure to law enforcement each time he logged on to his work computer. United States v. Greiner, 235 F. App'x 541, 542 (9th Cir. 2007).

*4 In this case, any expectation of privacy in Defendant's work email was objectively unreasonable under the military's computer-use policies in effect at his workplace. AR 25-2 specified that Defendant had "no expectation of privacy while using [information systems] or accessing Army resources." ECF 48-2. Additionally, both AR 25-2 and the Oregon National Guard's acceptable use policy stated that communications using Defendant's work computer were routinely monitored for law enforcement purposes. Id.; ECF 48-1 at 4. Unlike Heckenkamp, in which the network policy affirmed a "basic principle" of privacy, see 482 F.3d at 1147, the terms in effect here made it abundantly clear that Defendant's communications over his work computer system were not private.

Furthermore, Defendant received routine reminders that these policies were in place. He was required to sign the Oregon National Guard's policy before receiving computer access at work and recertified his understanding of its conditions each year. ECF 48 at 4–5. He also participated in the Defense Department's annual training, the "Cyber Awareness Challenge," which "advised users that there was no expectation of privacy in the use of [the Department's] systems." Id. at 5. Most importantly, he received notice of the policies via the warning banner displayed each time he accessed his work computer. Id. at 3. The Ninth Circuit has held that no reasonable expectation of privacy exists where this kind of warning banner provides "ample reason to be aware that [a defendant's] stored files and internet usage were subject to monitoring by his employer and disclosure to law enforcement personnel, and that by using the computer he was deemed to have consented to such monitoring and disclosure." Greiner, 235 F. App'x at 542. Thus, any expectation of privacy in Defendant's work email was objectively unreasonable here.

Nevertheless, Defendant contends that City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010), and United States v. Long, 64 M.J. 57 (C.A.A.F. 2006), support his claim of a reasonable expectation of privacy. In Quon, the Supreme Court assumed—but did not decide—that the defendant had a reasonable expectation of privacy in text messages sent over a pager provided by his government employer, despite policies which might have suggested otherwise. 560 U.S. at 758–65. And in Long, the Court of Appeals for the Armed Forces held that a member of the military had a reasonable expectation of privacy in emails sent from her military account despite a log-on banner warning of monitoring. 64 M.J. at 65.

Neither case requires suppression here. First, in Quon, the Supreme Court did not decide whether the defendant had a reasonable expectation of privacy: the extent of the workplace policies was ambiguous, and the Court decided the case on other grounds. See 560 U.S. at 758, 760. That uncertainty is not present here, where AR 25-2 unambiguously announced that Defendant had no expectation of privacy in the email account provided by his military employer. ECF 48-2. Second, Long underscores that the objective prong of Katz requires parsing the terms of the policies in place. Unlike in that case, where the policies described "very limited conditions" of monitoring, 64 M.J. at 64, both policies here informed Defendant that his communication would be monitored for law enforcement purposes. Under these circumstances, it was objectively unreasonable for Defendant to expect privacy in his work email.

CONCLUSION

For the reasons stated in this opinion and order, Defendant's motion to suppress, ECF 37, is DENIED.

IT IS SO ORDERED.

DATED this 6th day of November, 2019.

Footnotes

[1]

The Government notes that at "some point after June 2010, users out of compliance were locked out of their account until the acknowledgement was complete." ECF 48 at 5. Because it is not clear when the computer system began to lock out users who had not recertified, this Court does not rely on this stipulated fact in its analysis.

[2]

The policy at issue in Heckenkamp provided that "in general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to ... protect the integrity of the University and the rights and property of the state." 482 F.3d at 1147.

End of Document.